

WHAT IS CLAIMED IS:

- Sub
a1
1. A method of email access control, comprising the steps of:
- 5 receiving a personalized access ticket containing a sender's identification and a recipient's identification in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, at a
- 10 secure communication service for connecting communications between the sender and the receiver; and
- controlling accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized
- 15 access ticket at the secure communication service.
2. The method of claim 1, wherein at the controlling step the secure communication service authenticates the personalized access ticket presented by the sender, and
- 20 refuses a delivery of the email when the personalized access ticket presented by the sender has been altered.
3. The method of claim 2, wherein the personalized access ticket is signed by a secret key of a secure processing
- 25 device which issued the personalized access ticket, and at the controlling step the secure communication service authenticates the personalized access ticket by verifying a signature of the secure processing device in the personalized access ticket using a public key of the secure
- 30 processing device.
4. The method of claim 1, wherein at the receiving step the secure communication service also receives the sender's identification presented by the sender along with the
- 35 personalized access ticket, and at the controlling step the

secure communication service checks whether the sender's identification presented by the sender is contained in the personalized access ticket presented by the sender, and refuses a delivery of the email when the sender's

5 identification presented by the sender is not contained in the personalized access ticket presented by the sender.

5. The method of claim 1, wherein the personalized access ticket also contains a validity period indicating a period
10 for which the personalized access ticket is valid, and at the controlling step the secure communication service checks the validity period contained in the personalized access ticket presented by the sender and refuses a
15 delivery of the email when the personalized access ticket presented by the sender contains the validity period that has already been expired.

6. The method of claim 5, wherein the validity period of the personalized access ticket is set by a trusted third
20 party.

7. The method of claim 1, further comprising the step of:
issuing the personalized access ticket to the sender
at a directory service for managing an identification of
25 each registrant and a disclosed information of each registrant which has a lower secrecy than a personal information, in a state which is accessible for search by unspecified many, in response to search conditions specified by the sender, by using an identification of a
30 registrant whose disclosed information matches the search conditions as the recipient's identification and the sender's identification specified by the sender along with the search conditions.

35 8. The method of claim 1, further comprising the step of:

registering in advance the personalized access ticket containing an identification of a specific user from which a delivery of emails to a specific registrant is to be refused as the sender's identification and an
5 identification of the specific registrant as the recipient's identification, at the secure communication service;

wherein the controlling step the secure communication service refuses a delivery of the email from the sender
10 when the personalized access ticket presented by the sender is registered therein in advance at the registering step.

9. The method of claim 8, further comprising the step of:
deleting the personalized access ticket registered
15 at the secure communication service upon request from the specific registrant who registered the personalized access ticket at the registering step.

10. The method of claim 1, wherein the personalized access
20 ticket also contains a transfer control flag indicating whether or not the sender should be authenticated by the secure communication service, and at the controlling step, when the transfer control flag contained in the personalized access ticket indicates that the sender should
25 be authenticated, the secure communication service authenticates the sender's identification presented by the sender and refuses a delivery of the email when an authentication of the sender's identification fails.

30 11. The method of claim 10, wherein the authentication of the sender's identification is realized by a challenge/response procedure between the sender and the secure communication service.

35 12. The method of claim 10, wherein the transfer control

flag of the personalized access ticket is set by a trusted third party.

13. The method of claim 1, wherein the sender's
5 identification and the recipient's identification in the personalized access ticket are given by real email addresses of the sender and the recipient.

14. The method of claim 1, wherein the sender's
10 identification and the recipient's identification in the personalized access ticket are given by anonymous identifications of the sender and the recipient, where an anonymous identification of each user contains at least one fragment of an official identification of each user by
15 which each user is uniquely identifiable by a certification authority.

15. The method of claim 14, wherein the anonymous
identification of each user is an information containing
20 the at least one fragment of the official identification of each user which is signed by the certification authority using a secret key of the certification authority.

16. The method of claim 14, wherein the official
25 identification of each user is a character string uniquely assigned to each user by the certification authority and a public key of each user which are signed by a secret key of the certification authority.

30 17. The method of claim 14, further comprising the step of:

probabilistically identifying an identity of the sender by reconstructing the official identification of the sender by judging identity of a plurality of anonymous
35 identifications of the sender contained in a plurality of

personalized access tickets used by the sender.

18. The method of claim 1, wherein an anonymous
identification of each user that contains at least one
5 fragment of an official identification of each user by
which each user is uniquely identifiable by a certification
authority and a link information of each anonymous
identification by which each anonymous identification can
be uniquely identified are defined, and the sender's
10 identification and the recipient's identification in the
personalized access ticket are given by a link information
of the anonymous identification of the sender and a link
information of the anonymous identification of the
recipient.

19. The method of claim 1, wherein the link information of
each anonymous identification is an identifier uniquely
assigned to each anonymous identification by the
certification authority.

20. The method of claim 18, further comprising the step
of:
probabilistically identifying an identity of the
sender by reconstructing the official identification of the
25 sender by judging identity of a plurality of anonymous
identifications of the sender corresponding to the link
information contained in a plurality of personalized access
tickets used by the sender.

21. The method of claim 1, wherein the personalized access
ticket contains a single sender's identification and a
single recipient's identification in 1-to-1 correspondence.

22. The method of claim 1, wherein the personalized access
35 ticket contains a single sender's identification and a

plurality of recipient's identifications in 1-to-N
correspondence, where N is an integer greater than 1.

23. The method of claim 22, wherein one identification
5 among the single sender's identification and the plurality
of recipient's identifications is a holder identification
for identifying a holder of the personalized access ticket
while other identifications among the single sender's
identification and the plurality of recipient's
10 identifications are member identifications for identifying
members of a group to which the holder belongs.

24. The method of claim 23, further comprising the step
of:
15 issuing an identification of each user and an enabler
of the identification of each user indicating a right to
change the personalized access ticket containing the
identification of each user as the holder identification,
to each user at a certification authority, such that
20 prescribed processing on the personalized access ticket can
be carried out at a secure processing device only by a user
who presented both the holder identification contained in
the personalized access ticket and the enabler
corresponding to the holder identification to the secure
25 processing device.

25. The method of claim 24, wherein the certification
authority issues the enabler of the identification of each
user as an information indicating that it is the enabler
30 and the identification of each user itself which are signed
by a secret key of the certification authority.

26. The method of claim 24, wherein the prescribed
processing includes a generation of a new personalized
35 access ticket, a merging of a plurality of personalized

access tickets, a splitting of one personalized access ticket into a plurality of personalized access tickets, a changing of the holder of the personalized access ticket, changing of a validity period of the personalized access ticket, and a changing of a transfer control flag of the personalized access ticket.

27. The method of claim 26, wherein a special identification and a special enabler corresponding to the special identification which are known to all users are defined such that the generation of a new personalized access ticket and the changing of the holder of the personalized access ticket can be carried out by the holder of the personalized access ticket by using the special identification and the special enabler without using an enabler of a member identification.

28. The method of claim 27, wherein the special identification is defined to be capable of being used only as the holder identification of the personalized access ticket.

29. The method of claim 26, wherein a special identification which is known to all users is defined such that a read only attribute can be set to the personalized access ticket by using the special identification.

30. The method of claim 1, wherein at the controlling step, when the access right of the sender with respect to the recipient is verified according to the personalized access ticket, the secure communication service takes out the recipient's identification from the personalized access ticket by using the sender's identification presented by the sender, converts the mail by using a taken out recipient's identification into a format that can be

interpreted by a mail transfer function for actually carrying out a mail delivery processing, and gives the mail after conversion to the mail transfer function by attaching the personalized access ticket.

5

31. A method of email access control, comprising the steps of:

10 defining an official identification of each user by which each user is uniquely identifiable by a certification authority, and an anonymous identification of each user containing at least one fragment of the official identification; and

15 identifying each user by the anonymous identification of each user in communications for emails on a communication network.

20 32. The method of claim 31, wherein the anonymous identification of each user is an information containing the at least one fragment of the official identification of each user which is signed by the certification authority using a secret key of the certification authority.

25 33. The method of claim 31, wherein the official identification of each user is a character string uniquely assigned to each user by the certification authority and a public key of each user which are signed by a secret key of the certification authority.

30 34. The method of claim 31, further comprising the steps of:

35 receiving a personalized access ticket containing a sender's anonymous identification and a recipient's anonymous identification in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an intended

destination of the email, at a secure communication service for connecting communications between the sender and the receiver; and

controlling accesses between the sender and the
5 recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket at the secure communication service.

35. The method of claim 34, further comprising the step
10 of:

probabilistically identifying an identity of the sender at the secure communication service by reconstructing the official identification of the sender while judging identity of a plurality of anonymous
15 identifications of the sender contained in a plurality of personalized access tickets used by the sender.

36. The method of claim 31, wherein the defining step also defines a link information of each anonymous identification
20 by which each anonymous identification can be uniquely identified, and each anonymous identification also contains the link information of each anonymous identification.

37. The method of claim 36, wherein the link information
25 of each anonymous identification is an identifier uniquely assigned to each anonymous identification by the certification authority.

38. The method of claim 36, further comprising the steps
30 of:

receiving a personalized access ticket containing a link information of a sender's anonymous identification and a link information of a recipient's anonymous identification in correspondence, which is presented by a
35 sender who wishes to send an email to a recipient so as to

specify the recipient as an intended destination of the email, at a secure communication service for connecting communications between the sender and the receiver; and controlling accesses between the sender and the
5 recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket at the secure communication service.

39. The method of claim 38, further comprising the step
10 of:

probabilistically identifying an identity of the sender by reconstructing the official identification of the sender while judging identity of a plurality of anonymous identifications of the sender corresponding to the link
15 information contained in a plurality of personalized access tickets used by the sender.

40. A communication system realizing email access control, comprising:

20 a communication network to which a plurality of user terminals are connected; and

a secure communication service device for connecting communications between the sender and the receiver on the communication network, by receiving a personalized access
25 ticket containing a sender's identification and a recipient's identification in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, and controlling accesses between
30 the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized access ticket.

41. The system of claim 40, wherein the secure
35 communication service device authenticates the personalized

access ticket presented by the sender, and refuses a delivery of the email when the personalized access ticket presented by the sender has been altered.

5 42. The system of claim 41, further comprising:

a secure processing device for issuing the personalized access ticket which is signed by a secret key of the secure processing device;

10 wherein the secure communication service device authenticates the personalized access ticket by verifying a signature of the secure processing device in the personalized access ticket using a public key of the secure processing device.

15 43. The system of claim 40, wherein the secure communication service device also receives the sender's

identification presented by the sender along with the personalized access ticket, checks whether the sender's identification presented by the sender is contained in the
20 personalized access ticket presented by the sender, and refuses a delivery of the email when the sender's identification presented by the sender is not contained in the personalized access ticket presented by the sender.

25 44. The system of claim 40, wherein the personalized access ticket also contains a validity period indicating a period for which the personalized access ticket is valid, and the secure communication service device checks the validity period contained in the personalized access ticket
30 presented by the sender and refuses a delivery of the email when the personalized access ticket presented by the sender contains the validity period that has already been expired.

45. The system of claim 44, further comprising:

35 a trusted third party for setting the validity period

of the personalized access ticket.

46. The system of claim 40, further comprising:

5 a directory service device for managing an
identification of each registrant and a disclosed
information of each registrant which has a lower secrecy
than a personal information, in a state which is accessible
for search by unspecified many, and issuing the
personalized access ticket to the sender in response to
10 search conditions specified by the sender, by using an
identification of a registrant whose disclosed information
matches the search conditions as the recipient's
identification and the sender's identification specified by
the sender along with the search conditions.

15

47. The system of claim 40, wherein the secure
communication service device registers in advance the
personalized access ticket containing an identification of
a specific user from which a delivery of emails to a
20 specific registrant is to be refused as the sender's
identification and an identification of the specific
registrant as the recipient's identification, and refuses a
delivery of the email from the sender when the personalized
access ticket presented by the sender is registered therein
25 in advance.

48. The system of claim 47, wherein the secure
communication service device deletes the personalized
access ticket registered therein upon request from the
30 specific registrant who registered the personalized access
ticket.

49. The system of claim 40, wherein the personalized
access ticket also contains a transfer control flag
35 indicating whether or not the sender should be

authenticated by the secure communication service, and when the transfer control flag contained in the personalized access ticket indicates that the sender should be authenticated, the secure communication service device
5 authenticates the sender's identification presented by the sender and refuses a delivery of the email when an authentication of the sender's identification fails.

10 50. The system of claim 49, wherein the authentication of the sender's identification is realized by a challenge/response procedure between the sender and the secure communication service device.

15 51. The system of claim 49, further comprising a trusted third party for setting the transfer control flag of the personalized access ticket.

20 52. The system of claim 40, wherein the sender's identification and the recipient's identification in the personalized access ticket are given by real email addresses of the sender and the recipient.

25 53. The system of claim 40, further comprising:
a certification authority device for issuing an anonymous identification of each user which contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by the certification authority device;

30 wherein the sender's identification and the recipient's identification in the personalized access ticket are given by anonymous identifications of the sender and the recipient.

35 54. The system of claim 53, wherein the anonymous identification of each user is an information containing

the at least one fragment of the official identification of each user which is signed by the certification authority device using a secret key of the certification authority device.

5

56. The system of claim 53, wherein the secure communication service device probabilistically identifies an identity of the sender by reconstructing the official identification of the sender while judging identity of a plurality of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

wherein the sender's identification and the recipient's identification in the personalized access ticket are given by a link information of the anonymous identification of the sender and a link information of the anonymous identification of the recipient.

assigned to each anonymous identification by the
certification authority device.

59. The system of claim 57, wherein the secure
5 communication service device probabilistically identifies
an identity of the sender by reconstructing the official
identification of the sender while judging identity of a
plurality of anonymous identifications of the sender
corresponding to the link information contained in a
10 plurality of personalized access tickets used by the
sender.

60. The system of claim 40, wherein the personalized
access ticket contains a single sender's identification and
15 a single recipient's identification in 1-to-1
correspondence.

61. The system of claim 40, wherein the personalized
access ticket contains a single sender's identification and
20 a plurality of recipient's identifications in 1-to-N
correspondence, where N is an integer greater than 1.

62. The system of claim 61, wherein one identification
among the single sender's identification and the plurality
25 of recipient's identifications is a holder identification
for identifying a holder of the personalized access ticket
while other identifications among the single sender's
identification and the plurality of recipient's
identifications are member identifications for identifying
30 members of a group to which the holder belongs.

63. The system of claim 62, further comprising:
a certification authority device for issuing to each
user an identification of each user and an enabler of the
35 identification of each user indicating a right to change

the personalized access ticket containing the
identification of each user as the holder identification;
and

5 a secure processing device at which prescribed
processing on the personalized access ticket can be carried
out only by a user who presented both the holder
identification contained in the personalized access ticket
and the enabler corresponding to the holder identification
to the secure processing device.

10

64. The system of claim 63, wherein the certification
authority device issues the enabler of the identification
of each user as an information indicating that it is the
enabler and the identification of each user itself which
15 are signed by a secret key of the certification authority
device.

65. The system of claim 63, wherein the prescribed
processing includes a generation of a new personalized
20 access ticket, a merging of a plurality of personalized
access tickets, a splitting of one personalized access
ticket into a plurality of personalized access tickets, a
changing of the holder of the personalized access ticket,
changing of a validity period of the personalized access
25 ticket, and a changing of a transfer control flag of the
personalized access ticket.

66. The system of claim 65, wherein a special
identification and a special enabler corresponding to the
30 special identification which are known to all users are
defined such that the generation of a new personalized
access ticket and the changing of the holder of the
personalized access ticket can be carried out by the holder
of the personalized access ticket by using the special
35 identification and the special enabler without using an

enabler of a member identification.

67. The system of claim 66, wherein the special identification is defined to be capable of being used only
5 as the holder identification of the personalized access ticket.

68. The system of claim 65, wherein a special identification which is known to all users is defined such
10 that a read only attribute can be set to the personalized access ticket by using the special identification.

69. The system of claim 40, wherein when the access right of the sender with respect to the recipient is verified
15 according to the personalized access ticket, the secure communication service device takes out the recipient's identification from the personalized access ticket by using the sender's identification presented by the sender,
converts the mail by using a taken out recipient's
20 identification into a format that can be interpreted by a mail transfer function for actually carrying out a mail delivery processing, and gives the mail after conversion to the mail transfer function by attaching the personalized access ticket.

25

70. A communication system realizing email access control, comprising:

a certification authority device for defining an official identification of each user by which each user is
30 uniquely identifiable by the certification authority device, and an anonymous identification of each user which contains at least one fragment of the official identification; and

a communication network on which each user is
35 identified by the anonymous identification of each user in

75. The system of claim 70, wherein the certification authority device also defines a link information of each anonymous identification by which each anonymous
5 identification can be uniquely identified, and each anonymous identification also contains the link information of each anonymous identification.

76. The system of claim 75, wherein the link information
10 of each anonymous identification is an identifier uniquely assigned to each anonymous identification by the certification authority device.

77. The system of claim 75, further comprising:
15 a secure communication service device for connecting communications between the sender and the receiver on the communication network, by receiving a personalized access ticket containing a link information of a sender's
20 anonymous identification and a link information of a recipient's anonymous identification in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to specify the recipient as an
intended destination of the email, and controlling accesses between the sender and the recipient by verifying an access
25 right of the sender with respect to the recipient according to the personalized access ticket.

78. The system of claim 77, wherein the secure communication service device probabilistically identifies
30 an identity of the sender by reconstructing the official identification of the sender while judging identity of a plurality of link informations of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

35

79. A secure communication service device for use in a communication system realizing email access control, comprising:

a computer hardware; and
5 a computer software for causing the computer hardware to connect communications between the sender and the receiver, by receiving a personalized access ticket containing a sender's identification and a recipient's identification in correspondence, which is presented by a
10 sender who wishes to send an email to a recipient so as to specify the recipient as an intended destination of the email, and controlling accesses between the sender and the recipient by verifying an access right of the sender with respect to the recipient according to the personalized
15 access ticket.

80. The secure communication service device of claim 79, wherein the computer software causes the computer hardware to authenticate the personalized access ticket presented by
20 the sender, and refuse a delivery of the email when the personalized access ticket presented by the sender has been altered.

81. The secure communication service device of claim 80,
25 wherein the personalized access ticket is signed by a secret key of a secure processing device which issued the personalized access ticket, and the computer software causes the computer hardware to authenticate the personalized access ticket by verifying a signature of the
30 secure processing device in the personalized access ticket using a public key of the secure processing device.

82. The secure communication service device of claim 79, wherein the computer software causes the computer hardware
35 to also receive the sender's identification presented

by the sender along with the personalized access ticket,
check whether the sender's identification presented by the
sender is contained in the personalized access ticket
presented by the sender, and refuse a delivery of the email
5 when the sender's identification presented by the sender is
not contained in the personalized access ticket presented
by the sender.

83. The secure communication service device of claim 79,
10 wherein the personalized access ticket also contains a
validity period indicating a period for which the
personalized access ticket is valid, and the computer
software causes the computer hardware to check the validity
period contained in the personalized access ticket
15 presented by the sender and refuse a delivery of the email
when the personalized access ticket presented by the sender
contains the validity period that has already been expired.

84. The secure communication service device of claim 79,
20 wherein the computer software causes the computer hardware
to register in advance the personalized access ticket
containing an identification of a specific user from which
a delivery of emails to a specific registrant is to be
refused as the sender's identification and an
25 identification of the specific registrant as the
recipient's identification, at the secure communication
service device, and refuse a delivery of the email from the
sender when the personalized access ticket presented by the
sender is registered at the secure communication service
30 device in advance.

85. The secure communication service device of claim 84,
wherein the computer software causes the computer hardware
to delete the personalized access ticket registered at the
35 secure communication service device upon request from the

specific registrant who registered the personalized access ticket.

86. The secure communication service device of claim 79,
5 wherein the personalized access ticket also contains a transfer control flag indicating whether or not the sender should be authenticated by the secure communication service device, and when the transfer control flag contained in the personalized access ticket indicates that
10 the sender should be authenticated, the computer software causes the computer hardware to authenticate the sender's identification presented by the sender and refuse a delivery of the email when an authentication of the sender's identification fails.

15 87. The secure communication service device of claim 86, wherein the computer software causes the computer hardware to realize the authentication of the sender's identification by a challenge/response procedure between
20 the sender and the secure communication service device.

88. The secure communication service device of claim 79, wherein the sender's identification and the recipient's identification in the personalized access ticket are given
25 by anonymous identifications of the sender and the recipient, where an anonymous identification of each user contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by a certification authority, and the computer
30 software also causes the computer hardware to probabilistically identify an identity of the sender by reconstructing the official identification of the sender by judging identity of a plurality of anonymous identifications of the sender contained in a plurality of
35 personalized access tickets used by the sender.

89. The secure communication service device of claim 79,
wherein an anonymous identification of each user that
contains at least one fragment of an official
5 identification of each user by which each user is uniquely
identifiable by a certification authority and a link
information of each anonymous identification by which each
anonymous identification can be uniquely identified are
defined, the sender's identification and the recipient's
10 identification in the personalized access ticket are given
by a link information of the anonymous identification of
the sender and a link information of the anonymous
identification of the recipient, and the computer software
also causes the computer hardware to probabilistically
15 identify an identity of the sender by reconstructing the
official identification of the sender by judging identity
of a plurality of anonymous identifications of the sender
corresponding to the link information contained in a
plurality of personalized access tickets used by the
20 sender.

90. The secure communication service device of claim 79,
wherein when the access right of the sender with respect to
the recipient is verified according to the personalized
25 access ticket, the computer software causes the computer
hardware to take out the recipient's identification from
the personalized access ticket by using the sender's
identification presented by the sender, convert the mail by
using a taken out recipient's identification into a format
30 that can be interpreted by a mail transfer function for
actually carrying out a mail delivery processing, and give
the mail after conversion to the mail transfer function by
attaching the personalized access ticket.

35 91. A secure processing device for use in a communication

system realizing email access control, comprising:

a computer hardware; and

a computer software for causing the computer hardware to receive a request for a personalized access ticket from a user, and issue a personalized access ticket containing a sender's identification and a recipient's identification in correspondence, which is signed by a secret key of the secure processing device.

92. A directory service device for use in a communication system realizing email access control, comprising:

a computer hardware; and

a computer software for causing the computer hardware to manage an identification of each registrant and a disclosed information of each registrant which has a lower secrecy than a personal information, in a state which is accessible for search by unspecified many, and issue a personalized access ticket containing a sender's identification and a recipient's identification in correspondence, to the sender in response to search conditions specified by the sender, by using an identification of a registrant whose disclosed information matches the search conditions as the recipient's identification and the sender's identification specified by the sender along with the search conditions.

93. A certification authority device for use in a communication system realizing email access control, comprising:

a computer hardware; and

a computer software for causing the computer hardware to issue to each user an official identification of each user by which each user is uniquely identifiable by the certification authority device, and an anonymous identification of each user which contains at least one

program code means embodied therein for causing a computer to function as a secure communication service device for use in a communication system realizing email access control, the computer readable program code means includes:

5 first computer readable program code means for causing said computer to receive a personalized access ticket containing a sender's identification and a recipient's identification in correspondence, which is presented by a sender who wishes to send an email to a recipient so as to
10 specify the recipient as an intended destination of the email; and

second computer readable program code means for causing said computer to control accesses between the sender and the recipient by verifying an access right of
15 the sender with respect to the recipient according to the personalized access ticket, so as to connect communications between the sender and the receiver on the communication network.

20 97. The computer usable medium of claim 96, the second computer readable program code means causes said computer to authenticate the personalized access ticket presented by the sender, and refuse a delivery of the email when the personalized access ticket presented by the sender has been
25 altered.

98. The computer usable medium of claim 97, wherein the personalized access ticket is signed by a secret key of a secure processing device which issued the personalized
30 access ticket, and the second computer readable program code means causes said computer to authenticate the personalized access ticket by verifying a signature of the secure processing device in the personalized access ticket using a public key of the secure processing device.

35

99. The computer usable medium of claim 96, wherein the first computer readable program code means causes said computer to also receive the sender's identification presented by the sender along with the personalized access ticket, and the second computer readable program code means causes said computer to check whether the sender's identification presented by the sender is contained in the personalized access ticket presented by the sender and refuse a delivery of the email when the sender's identification presented by the sender is not contained in the personalized access ticket presented by the sender.

100. The computer usable medium of claim 96, wherein the personalized access ticket also contains a validity period indicating a period for which the personalized access ticket is valid, and the second computer readable program code means causes said computer to check the validity period contained in the personalized access ticket presented by the sender and refuse a delivery of the email when the personalized access ticket presented by the sender contains the validity period that has already been expired.

101. The computer usable medium of claim 96, wherein the second computer readable program code means causes said computer to register in advance the personalized access ticket containing an identification of a specific user from which a delivery of emails to a specific registrant is to be refused as the sender's identification and an identification of the specific registrant as the recipient's identification, at the secure communication service device, and refuse a delivery of the email from the sender when the personalized access ticket presented by the sender is registered at the secure communication service device in advance.

35

102. The computer usable medium of claim 101, wherein the second computer readable program code means causes said computer to delete the personalized access ticket registered at the secure communication service device upon request from the specific registrant who registered the personalized access ticket.

103. The computer usable medium of claim 96, wherein the personalized access ticket also contains a transfer control flag indicating whether or not the sender should be authenticated by the secure communication service device, and when the transfer control flag contained in the personalized access ticket indicates that the sender should be authenticated, the second computer readable program code means causes said computer to authenticate the sender's identification presented by the sender and refuse a delivery of the email when an authentication of the sender's identification fails.

104. The computer usable medium of claim 103, wherein the second computer readable program code means causes said computer to realize the authentication of the sender's identification by a challenge/response procedure between the sender and the secure communication service device.

105. The computer usable medium of claim 96, wherein the sender's identification and the recipient's identification in the personalized access ticket are given by anonymous identifications of the sender and the recipient, where an anonymous identification of each user contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by a certification authority, and the second computer readable program code means also causes said computer to probabilistically identify an identity of the sender by reconstructing the

official identification of the sender by judging identity of a plurality of anonymous identifications of the sender contained in a plurality of personalized access tickets used by the sender.

5

106. The computer usable medium of claim 96, wherein an anonymous identification of each user that contains at least one fragment of an official identification of each user by which each user is uniquely identifiable by a certification authority and a link information of each anonymous identification by which each anonymous identification can be uniquely identified are defined, the sender's identification and the recipient's identification in the personalized access ticket are given by a link information of the anonymous identification of the sender and a link information of the anonymous identification of the recipient, and the second computer readable program code means also causes said computer to probabilistically identify an identity of the sender by reconstructing the official identification of the sender by judging identity of a plurality of anonymous identifications of the sender corresponding to the link information contained in a plurality of personalized access tickets used by the sender.

25

107. The computer usable medium of claim 96, wherein when the access right of the sender with respect to the recipient is verified according to the personalized access ticket, the second computer readable program code means causes said computer to take out the recipient's identification from the personalized access ticket by using the sender's identification presented by the sender, convert the mail by using a taken out recipient's identification into a format that can be interpreted by a mail transfer function for actually carrying out a mail

35

delivery processing, and give the mail after conversion to the mail transfer function by attaching the personalized access ticket.

5 108. A computer usable medium having computer readable program code means embodied therein for causing a computer to function as a secure processing device for use in a communication system realizing email access control, the computer readable program code means includes:

10 first computer readable program code means for causing said computer to receive a request for a personalized access ticket from a user; and

second computer readable program code means for causing said computer to issue the personalized access
15 ticket containing a sender's identification and a recipient's identification in correspondence, which is signed by a secret key of the secure processing device.

109. A computer usable medium having computer readable
20 program code means embodied therein for causing a computer to function as a directory service devicer for use in a communication system realizing email access control, the computer readable program code means includes:

first computer readable program code means for causing
25 said computer to manage an identification of each registrant and a disclosed information of each registrant which has a lower secrecy than a personal information, in a state which is accessible for search by unspecified many, and

30 second computer readable program code means for causing said computer to issue a personalized access ticket containing a sender's identification and a recipient's identification in correspondence, to the sender in response to search conditions specified by the sender, by using an
35 identification of a registrant whose disclosed information

holder identification.

112. A computer usable medium having computer readable program code means embodied therein for causing a computer to function as a secure processing device for use in a communication system realizing email access control, the computer readable program code means includes:

first computer readable program code means for causing said computer to receive from a user a request for prescribed processing on a personalized access ticket containing a sender's identification and a plurality of recipient's identifications in correspondence, where one of the sender's identification and the recipient's identifications is a holder identification; and

second computer readable program code means for causing said computer to execute the prescribed processing on the personalized access ticket when the user presented both the holder identification contained in the personalized access ticket and an enabler corresponding to the holder identification which indicates a right to change the personalized access ticket containing the identification of the user as the holder identification.